COMITÉ PERMANENT DE CONTROLE DES SERVICES DE RENSEIGNEMENT ET DE SECURITE

Numéro de notice : 2022.295

Analyse juridique des possibilités légales dont disposent les deux services de renseignement en matière d'entrave

20 janvier 2023

TABLE DES MATIÈRES

Le présent document renferme une analyse juridique de la théorie de la disruption de la VSSE et formule un certain nombre de recommandations à orientation juridique. En outre, ce document aborde les capacités d'action juridique du SGRS dans le cadre de l'entrave des menaces pour la sécurité, avec un accent particulier sur les cybercapacités offensives du renseignement militaire. Il y a lieu de préciser que les différents termes utilisés pour nommer le phénomène, à savoir « disruption », « entrave » et « perturbation », revêtent la même signification.

ORIGINE DE L'ENQUÊTE

Le présent rapport est une analyse juridique du Comité permanent R des options légales dont disposent les services de renseignement en matière d'entrave (ou disruption). Il vise à clarifier une question qui a été de plus en plus soulevée dans divers dossiers examinés par le Comité, notamment l'enquête de contrôle sur la manière dont la Sûreté de l'État a assuré le suivi de l'imam Mohamed TOJGANI.[1] Même dans le contexte du contrôle exercé par le Comité dans le cadre de sa mission en tant qu'autorité de protection des données (APD) à l'égard de la VSSE et du SGRS, en particulier dans le cadre du traitement des dossiers de plaintes APD, cette question revient au premier plan au compte-gouttes.

Enfin, le présent rapport développe et approfondit la recommandation du Comité relative à l'entrave. Cette recommandation est issue de l'enquête de contrôle sur le suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes concernant les services de renseignement et de sécurité.[2]

PARTIE I. ENTRAVE PAR LA VSSE

1.1 ORIGINE DE LA THÉORIE DE LA DISRUPTION

La théorie de la disruption dans le domaine du renseignement belge trouve son origine dans la note du 31 août 2016 de l'Administrateur général de la Sûreté de l'État adressée au Président de la Commission d'enquête parlementaire Attentats terroristes.[3] Par cette note, la VSSE entendait informer les membres et les experts de la Commission d'enquête de divers sujets et questions, y compris de son point de vue sur la perturbation des menaces pour la sécurité.[4] Le service de renseignement y affirme que : *"De VSSE is er zich van bewust dat in de huidige nationale en internationale situatie, waar de terreurdreiging nog nooit zo groot is geweest, de rol van de dienst niet beperkt kan blijven tot het louter informeren van de bevoegde autoriteiten. [De VSSE] is […] vragende partij voor een duidelijkere definiëring van de eigen rol en verantwoordelijkheid op het vlak van de strijd tegen radicalisering en terrorisme. De dienst is ook vragende partij om meer verantwoordelijkheid op te nemen in*

1 COMITÉ PERMANENT R, « Enquête de contrôle sur la manière dont la Sûreté de l'État a assuré le suivi de l'imam Mohamed TOJGANI ».

2 COMITÉ PERMANENT R, « Enquête de contrôle relative au suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes concernant les services de renseignement et de sécurité », p. 13.

3 Cette note de la VSSE du 31 août 2016 est également adressée au ministre de la Justice, au ministre de l'Intérieur et au Président du Comité permanent R.

4 Pour la section traitant de la théorie de la disruption, voir : p. 24 à 26.

deze, met name wat betreft disruptie van extremistische en terroristische activiteiten.".[5] Lors de son audition, le 5 octobre 2016, devant la Commission d'enquête parlementaire, l'Administrateur général de la VSSE a largement réitéré ce qui avait déjà été communiqué dans la note précitée.[6]

Dans son Troisième Rapport intermédiaire du 15 juin 2017 traitant le volet « architecture de la sécurité », la Commission d'enquête parlementaire s'est ralliée à l'avis de la VSSE en ces termes : *« La Belgique part généralement du principe que les services de renseignement jouent essentiellement un rôle d'information qui se traduit par la transmission de renseignements aux autres services publics. La commission d'enquête estime qu'il conviendrait de confier des responsabilités plus étendues à la VSSE dans le domaine de la lutte contre la radicalisation, de l'extrémisme et du terrorisme. Sur ce point, la commission d'enquête se rallie à la théorie de la disruption proposée par l'administrateur général de la VSSE. Elle estime qu'il convient effectivement de permettre à la VSSE de perturber suffisamment certaines activités nuisibles pour qu'elles n'aient plus lieu, ou du moins pour réduire leur nocivité. »*.[7]

L'étape ultérieure de la théorie de la disruption se situe en 2018. Alors qu'en 2016 la VSSE est encore demandeuse de davantage de responsabilités en matière de disruption des activités extrémistes et terroristes, deux ans plus tard, c'est le service de renseignement qui prend l'initiative. Ainsi, en novembre 2018, circule au sein de la VSSE une note de service (classifiée) qui établit et détaille les procédures de perturbation au sein du service de renseignement.[8] Une attention particulière est accordée aux aspects tels que le moment où la VSSE s'engage dans la perturbation ainsi que la manière dont la perturbation de la menace doit être intégrée – de manière procédurale – dans le travail de renseignement. Ces procédures ont été actualisées en 2020[9], en tentant compte des réformes digitales au sein de la VSSE, tout en gardant à l'esprit les réformes en cours autour du modèle d'investigation à mettre en place dans le cadre du travail de renseignement (*'investigative model'*).

Outre la Commission d'enquête parlementaire Attentats terroristes, le Conseil national de sécurité demande et exige également que l'on accorde plus d'attention à la perturbation des menaces pour la sécurité de l'État. Dans sa (première) stratégie de sécurité nationale datée du 1er décembre 2021, il déclare : *« En raison de son statut de pays hôte de diverses*

---

5 *« La VSSE est consciente que dans la situation nationale et internationale actuelle, où la menace terroriste n'a jamais été aussi grande, son rôle ne peut se limiter à simplement informer les autorités compétentes. [La VSSE] demande [...] une définition plus claire de son propre rôle et de sa responsabilité en matière de lutte contre la radicalisation et le terrorisme. Le service est également appelé à assumer davantage de responsabilités à cet égard, notamment en ce qui concerne la perturbation des activités extrémistes et terroristes. »* (traduction libre).

6 Annexe n°1 du Troisième Rapport intermédiaire sur le volet "architecture de la sécurité" fait au nom de la Commission d'enquête parlementaire (…) – Rapports intégraux des réunions publiques, *Doc. parl.*, Chambre, 2015-2016, n° 54-1752/008, p. 102-137.

7 Troisième Rapport intermédiaire sur le volet "architecture de la sécurité" fait au nom de la Commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste, *Doc. parl.*, Chambre, 2015-2016, n° 54-1752/008, p. 308-309.

8 Note de service n° 18-50 du 5 november 2018 de l'Administrateur général de la VSSE relative aux procédures concernant l'entrave primaire et secondaire.

9 Note de service n° 20-29 du 11 juin 2020 de l'Administrateur général de la VSSE relative à l'actualisation des procédures concernant la disruption primaire et secondaire (non classifiée, diffusion restreinte).

institutions européennes et du siège de l'OTAN, la Belgique constitue un pôle d'attraction pour l'espionnage et l'ingérence. Afin de lutter contre cette menace, les services de renseignement visent avant tout à créer un environnement opérationnel hostile (hostile operating environment) pour les agents de renseignement étrangers. Les représentants politiques et diplomatiques doivent être pleinement sensibilisés au danger et ensuite être armés contre celui-ci. Une culture de la sécurité voit ainsi le jour au niveau national, qui assure la résilience nécessaire face à la menace d'espionnage et d'ingérence. ».[10]

Le Comité permanent R constate que des objectifs stratégiques sont formulés par diverses autorités politiques à l'égard de la VSSE et que des attentes ont été créées en termes de perturbation des menaces pour la sécurité nationale. À ce jour, toutefois, aucune intervention législative n'a eu lieu dans le cadre de la mise en œuvre de la théorie de la disruption. Il convient de mentionner ici que la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après : Loi Renseignement ou L.R&S) a déjà été largement modifiée à deux reprises depuis l'audition de l'Administrateur général de la VSSE devant la Commission d'enquête. Cependant, ni la Loi du 30 mars 2017[11] ni la Loi du 14 juillet 2022[12] n'ont apporté de modifications à la Loi Renseignement en ce qui concerne la théorie de la disruption. La Commission d'accompagnement avait pourtant recommandé que *« [c]ompte tenu des répercussions des interventions dirusptives sur les droits des personnes ou des entités visées, la commission d'enquête estime qu'il est essentiel de prévoir les garanties juridiques nécessaires. Ces interventions doivent donc se fonder sur une base juridique qui doit encore être créée. Il faudra non seulement y définir les conditions d'application de ces interventions, mais également y prévoir les mécanismes de contrôle nécessaires. »*.[13] Ainsi, la Commission d'enquête a jugé indispensable de souligner – à deux reprises – que la VSSE doit se voir attribuer davantage de pouvoirs en matière de perturbation des menaces, mais qu'il y a lieu de fixer *« garanties juridiques nécessaires »* dans une loi formelle. En d'autres termes, la poursuite de l'élaboration de la théorie de la perturbation doit, selon la Commission d'enquête parlementaire, être précédée d'un débat parlementaire.

Dans le présent rapport, le Comité se penche, dans la première partie, sur la manière dont la VSSE organise sa théorie de la disruption en interne. Le Comité se concentre ici sur le cadre réglementaire interne et examine s'il est adéquat à la lumière du cadre légal et conventionnel applicable à la VSSE. Le Comité n'a pas examiné comment le service de renseignement civil met en pratique sa théorie de la disruption à ce stade. Bien que la théorie de la disruption trouve son origine à la VSSE, la seconde partie examine comment le Service Général du Renseignement et de la Sécurité (SGRS) est autorisé à combattre et à entraver les menaces à la sécurité.

---

10 Stratégie de sécurité nationale du 1er décembre 2021, p. 38 (www.premier.be).

11 Loi du 30 mars 2017 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal (*M.B.* 28 avril 2017).

12 Loi du 14 juillet 2022 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal (*M.B.* 5 août 2022).

13 *Doc. parl.*, Chambre, 2015-2016, n° 54-1752/008, p. 56 et 308.

1.2 DESCRIPTION ET CONTEXTUALISATION DE LA NOTION DE DISRUPTION

1.2.1 Nature et finalité de la disruption

La VSSE décrit la 'disruption' comme suit : *« l'entrave est la perturbation des menaces de sorte qu'elle ne se produise plus ou d'en réduire considérablement la nocivité »*.[14] Une distinction est établie entre la disruption primaire (ou disruption de première ligne) et la disruption secondaire (ou disruption de deuxième ligne). La disruption primaire comprend *« les mesures exécutées par la VSSE elle-même (sans la coopération de partenaires externes) afin d'entraver une menace »*. La disruption secondaire est *« le résultat d'une transmission de données de renseignement par la VSSE à une instance (publique) qui de son propre chef prendra des mesures afin d'entraver une menace »*.[15]

La finalité des mesures d'entrave définie par la VSSE est décrite comme suit : *« [a]vec la prévention et le conseil, l'entrave forme une réponse au souhait de la direction d'activer les renseignements d'une part, et de donner le rôle le plus (inter)actif souhaité par les 'clients' de la VSSE d'autre part. En outre, l'entrave est une condition sine qua non pour un travail davantage basé sur des projets selon le modèle d'investigation. La réalisation plus cohérente de la vision 'Prévenir – Conseiller – Entraver' dans les différentes missions de la VSSE devrait en effet permettre à la VSSE de fournir une réponse à la menace, même avec des moyens limités »*.[16] La VSSE précise encore que *« [t]out le travail que la VSSE réalise peut […] avoir un effet entravant"*, mais que par disruption on entend *« les actions qui sont entreprises avec l'intention d'entraver et pour lesquelles l'entrave constitue la finalité. »*.[17]

Dans sa note du 31 août 2016 adressée à la Commission d'enquête parlementaire, la VSSE précise que *« [l]a disruption [...] peut viser à la fois les individus qui développent des activités nuisibles et d'autres entités qui sont à l'origine d'activités nuisibles ou qui s'y livrent, comme les librairies radicales ou les établissements d'enseignement extrémistes. Au niveau macro, il peut même s'agir de pays tiers qui sont, d'une manière ou d'une autre, impliqués dans la diffusion de l'extrémisme (ou – plus hypothétiquement – du terrorisme). »*.

Cette description (interne) indique clairement que la disruption se situe dans le cadre de l'utilisation ciblée des renseignements collectés et traités par la VSSE. La perturbation secondaire implique l'utilisation des renseignements par les instances (publiques) auxquelles le service a transmis ses renseignements. La VSSE fournira ses renseignements à des instances et des individus tiers avec pour objectif spécifique que ces derniers, à partir de leurs propres attributions et lignes d'action, prennent des mesures visant à perturber une menace identifiée par la VSSE. En d'autres termes, la VSSE ne se contentera pas d'avertir les instances tierces des menaces pour la sécurité, mais elle leur proposera également de prendre des mesures spécifiques visant à neutraliser ou à faire échouer ces menaces. Des exemples typiques de ces contre-mesures : retrait par l'Office des étrangers du permis de séjour d'un étranger agissant sur le territoire belge en tant qu'agent d'un service de renseignement étranger, déclarer persona non grata un diplomate étranger espion, prendre un arrêté ou une

[14] Cette définition figure dans les notes de service n° 18-50 et n° 20-29. Elle a cependant été consignée pour la première fois dans la note VSSE du 31 août 2016 adressée à la Commission d'enquête parlementaire.
[15] Note de service n° 20-29, p. 1.
[16] Note de service n° 18-50, p. 1-2.
[17] *Ibid*.

mesure disciplinaire à l'encontre d'un fonctionnaire belge espion, et poursuivre et juger un terroriste ou un extrémiste sur la base de l'arsenal de sanctions existant.

Quant à l'entrave primaire, elle implique l'utilisation par la VSSE elle-même des renseignements qu'elle produit (*intelligence*). La VSSE ne se comporte plus comme un service de renseignement chargé de détecter et de surveiller les menaces, mais plutôt comme un service d'action chargé de contrer réellement les menaces. En d'autres termes, la VSSE prend elle-même les contre-mesures qu'elle juge nécessaires.

Dans le cadre de la description de la nature et de la finalité de la disruption, il convient de mentionner l'objectif du travail de renseignement décrit précédemment par le gouvernement: *« la finalité de la mission de renseignement consiste en l'identification et le contrôle de phénomènes, groupements et personnes qui présentent ou pourraient présenter une menace de sécurité spécifique. En d'autres mots, il s'agit tant de la détection, du suivi, de la maîtrise de menaces (ou risques) potentielles que du suivi et de la maîtrise de menaces (ou dangers) déjà détectées. ».*[18] Cette gestion des menaces déjà détectées correspond clairement à la prise de mesures d'entrave. La question centrale est ici de savoir sous quelle forme, dans quels cas et dans quelles conditions cette activité doit avoir lieu, ainsi qu'avec quelles restrictions et interdictions. Comme nous le précisons ci-dessous, pour formuler une réponse à cette question, il convient non seulement de tenir compte du cadre juridique applicable à la VSSE et, par extension, au SGRS (par ex. la Loi Renseignement[19], la Loi relative à la Protection des données[20], la Loi relative à la Classification[21]), mais également du cadre conventionnel applicable aux deux services de renseignement (par ex. CEDH[22]).

Enfin, il convient d'attirer l'attention sur le fait que la VSSE décrit l'entrave comme une condition nécessaire à un travail plus axé sur les projets selon le *Investigative model*. Conformément à son Plan stratégique 2021-2024, la VSSE travaille actuellement sur un nouveau « modèle d'investigation » – appelé *Investigative model* – qui entrera en vigueur à partir de mars 2023 pour toutes les menaces relevant de sa compétence. Ce modèle suppose un traitement immédiat des nouveaux leads[23] dans une REDDbox (*Read-Evaluate-Develop-Decide* box). *« Le lead est évalué immédiatement sur la base de certains critères et si les critères enregistrent un score élevé, le lead en question fait l'objet d'un traitement plus rapide et plus approfondi ».*[24] [25] Un des objectifs centraux du modèle d'investigation à introduire est que la VSSE souhaite travailler de manière plus ciblée vers les objectifs, non seulement en

---

[18] Exposé des motifs de la Loi du 30 mars 2017, *Doc. parl,.* Chambre 2015-2016, n° 54-2043/001, p.59.

[19] Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (*M.B.* 18 décembre 1998 – en abrégé : Loi Renseignement ou L.R&S).

[20] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (*M.B.* 5 septembre 2018).

[21] Loi du 11 décembre 1998 relative à la classificiation et aux habilitations, attestations et avis de sécurité (*M.B.* 7 mai 1999).

[22] La Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et libertés fondamentales, signée à Rome et approuvée par la loi du 13 mai 1955 (*M.B.* 19 août 1955, *err. M.B.* 29 juin 1961).

[23] Un *lead* est une information relative à une menace.

[24] Rapport global « État des lieux des recommandations en matière de Justice, Commission d'enquête parlementaire attentats du 22 mars », par le ministre de la Justice le 18 mars 2022, Recommandation 43 pour la VSSE.

[25] COMITÉ PERMANENT R, « Enquête de contrôle relative au suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes concernant les services de renseignement et de sécurité », p. 13.

lançant et en menant une enquête de renseignement, mais également en utilisant par la suite les résultats de l'enquête obtenus. Ou, comme le dit la VSSE elle-même dans sa communication à la Commission d'enquête parlementaire Attentats terroristes : *"De VSSE is er zich van bewust dat in de huidige nationale en internationale situatie, waar de terreurdreiging nog nooit zo groot is geweest, de rol van de dienst niet beperkt kan blijven tot het louter informeren van de bevoegde autoriteiten."*.[26] [27] Et ensuite : "*Als wij tot nu toe onze rol vaak beperkten tot het louter informeren van de autoriteiten, dan denk ik dat wij nu actiever moeten proberen te communiceren inzake de inlichtingen die door onze dienst kunnen worden verstrekt. Eventueel kunnen die vergezeld gaan van een soort van beleidsadvies, waarbij wij bepaalde zaken aanraden om te doen."*.[28] [29] La note de service interne « disruption » de 2018 – et son actualisation en 2020 – élargit la manière dont la VSSE souhaite jouer un rôle plus actif, et ce non seulement dans le cadre de la communication externe aux partenaires du service de renseignement (*cf.* disruption secondaire), mais aussi dans le cadre de sa propre action exécutive (*cf.* disruption primaire).

1.2.2 Description légale

La 'disruption' est un concept politique et opérationnel qui nécessite une traduction juridique afin de déterminer les interdictions et les restrictions qui régissent ces activités ainsi que les réglementations qui, le cas échéant, font défaut.

DISRUPTION SECONDAIRE

D'un point de vue juridique, une mesure de disruption secondaire consiste, pour la VSSE, à communiquer des renseignements à des instances et individus tiers conformément à la réglementation juridique qui s'applique. Les renseignements peuvent être communiqués tant à une instance (publique) belge (via une NA), l'Office des étrangers, la Diplomatie et le Ministère public occupant une position particulière, qu'à un service de renseignement et de sécurité étranger (via une NE).

La communication des renseignements de la VSSE est réglé en ordre principal par l'article 19, alinéa 1er L.R&S.[30] Cet article dispose que : *"(l)es services de renseignement et de sécurité ne*

---

[26] Note du 31 août 2016 de l'Administateur général de la VSSE au Président de la Commission d'enquêtes Attentats, aux ministres de la Justice et de l'Intérieur et au Président du Comité permanent R, p. 24 (concernant le projet de disprution).

[27] *« La VSSE est consciente que dans la situation nationale et internationale actuelle, où la menace terroriste n'a jamais été aussi grande, son rôle ne peut se limiter simplement informer des autorités compétentes »* (traduction libre).

[28] Audition du 5 octobre 2016 de l'Administrateur général de la VSSE à la Commission d'enquête parlementaire sur les attentats terroristes, Annexe n°1 du Troisième Rapport intermédiaire sur le volet "architecture de la sécurité" fait au nom de la Commission d'enquête parlementaire (…) – Rapports intégraux des réunions publiques, *Doc. parl.,* Chambre, 2015-2016, n° 54-1752/008, p. 102-137 (118).

[29] *« Si jusqu'à présent nous avons souvent limité notre rôle à la simple information des autorités, je pense que nous devrions maintenant essayer de communiquer plus activement sur les renseignements que peut fournir notre service. Ils pourraient éventuellement être accompagnés d'une sorte d'avis sur la politique à suivre, dans lequel nous recommandons certaines choses à faire. »* (traduction libre).

[30] D'autres dispositions légales réglementant la communication de renseignements et de données à caractère personnel à des instances tierces concernent par exemple l'art. 29 du Code d'instuction criminelle, l'art. 19/1

communiquent les renseignements visés à l'article 13, deuxième alinéa, » – en d'autres termes, les informations traitées ('renseignements' ou 'intelligence') relatives aux menaces pour la sécurité qui relèvent de la compétence matérielle de la VSSE – *« qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée [à l'article] 7 […] »*. Ces menaces comprennent le terrorisme, l'extrémisme, l'espionnage, l'ingérence, la prolifération des armes de destruction massive, les organisations criminelles et les sectes nuisibles.

Bien que les catégories de destinataires soient largement définies, il est néanmoins important que l'article 19, alinéa 1er L.R&S constitue une liste exhaustive de destinataires (voir la formulation *« ne communiquent […] qu'aux »*). Il est également important ici que *« les instances et personnes qui font l'objet d'une menace »* puissent être les destinataires des renseignements de la VSSE.

L'article 19, alinéa 1er L.R&S doit être lu conjointement avec l'article 20, §§ 1er et 3 L.R&S. Ce dernier stipule que :

> *« § 1er. Les services de renseignement et de sécurité, les services de police, les autorités administratives et judiciaires veillent à assurer entre eux une coopération mutuelle aussi efficace que possible. Les services de renseignement et de sécurité veillent également à assurer une collaboration avec les services de renseignement et de sécurité étrangers. »*
>
> *« § 3.* ***Le Comité ministériel définit les conditions de la communication prévue à l'article 19, alinéa 1er, et de la coopération prévue au § 1er du présent article.*** *».*

Le Comité constate qu'il n'existe pas de directives particulières du Conseil national de sécurité (CNS) réglementant la communication et la transmission de renseignements dans les actions *« qui sont entreprises avec l'intention d'entraver et pour lesquelles l'entrave constitue la finalité »* (*cf*. l'objectif spécifique d'une communication et d'une transmission de renseignements par la VSSE à une instance tierce, telle que définie par l'Administrateur général de la VSSE dans la note de service interne de la VSSE n° 18-50).

La mise en œuvre partielle de l'obligation légale visée à l'article 20, § 3 L.R&S figure dans la Directive non publique du 16 février 2000 concernant la communication de renseignements et la coopération entre les services de renseignement et de sécurité et les autorités et services administratifs' (directive CNS autorités BE). En outre, il existe la directive non publique du 30 septembre 2016 portant sur les relations de la Sûreté de l'État (VSSE) et du Service Général du Renseignement et de la Sécurité (SGRS) avec les services de renseignement étrangers' (CNS – directive Services de renseignement étrangers).[31]

Le Comité estime qu'aucune des deux directives du CNS n'est suffisamment élaborée pour répondre aux exigences de l'article 20, § 3 L.R&S. Le Comité reconnaît que la directive du CNS sur les Services de renseignement étrangers est beaucoup plus complète que la directive du SNC sur les autorités BE. Dans le premier cas, le Conseil national de sécurité pourrait se limiter

---

L.R&S, l'art. 6 Loi OCAM, l'article 21, § 5 Code de la nationalité belge, et les art. 44/2, § 2 et 44/11/3*ter*, § 4 LFP *i.o.* art. 7, § 1er, alinéa 1er AR Terrorist Fighters et art. 7, § alinéa 1er, AR Propagandistes de haine.

[31] Les circulaires ministérielles, après avoir été consultées et approuvées par le Conseil national de sécurité, peuvent également mettre en œuvre l'exigence légale visée à l'article 20, § 3 L.R&S. Cette procédure est généralement appliquée dans le cadre du suivi de phénomènes de sécurité spécifiques. Un exemple : la circulaire ministérielle Terrorist fighters et Propagandistes de la haine du 22 mai 2018.

à une annexe à la directive existante. Toutefois, cette dernière est tellement datée et si peu concrète qu'une révision globale s'impose.

Enfin, il est important de noter que ni l'article 19 L.R&S ni aucune autre disposition de la loi ne prévoient la possibilité que les instances et les personnes dont émane la menace soient informées que la VSSE les suit ou les a suivies.[32] L'obligation de confidentialité réglée à l'article 36 L.R&S prévoit par ailleurs que le secret – par exemple le fait que la VSSE détient un dossier sur la personne concernée – ne peut être transmis qu'à l'extérieur en vertu de l'article 19 L.R&S.[33] Dans ce contexte, **la question se pose, entre autres, de savoir sur quelle base juridique la VSSE peut, par exemple, notifier à une cible (individu ou service étranger) qu'elle est suivie par le service et l'avertir de la fin de l'opération de suivi.**

DISRUPTION PRIMAIRE

D'un point de vue juridique, la principale mesure de disruption primaire est l' 'utilisation' par la VSSE elle-même des renseignements qu'elle produit. Comme cela a été mentionné, la VSSE ne se comportera alors plus comme un service de renseignement chargé de détecter et de surveiller les menaces, mais plutôt comme un service d'action chargé de combattre réellement les menaces.

Traditionnellement, le travail de renseignement distingue quatre types d'activités : la collecte d'informations, le traitement des informations, l'analyse des renseignements et la communication des renseignements. Juridiquement, nous retrouvons ces quatre catégories d'activités de renseignement dans la définition légale de la mission de renseignement. Tant l'article 7, 1° L.R&S (mission de renseignement générale) que l'article 3°/1 L.R&S (mission de renseignement spécifique) stipulent que la VSSE a pour mission *« de rechercher, d'analyser et de traiter le renseignement »*.

De lege lata, il n'existe aucune disposition légale réglementant ou couvrant les mesures de disruption primaire de la VSSE. Comme mentionné, les deux dispositions légales susmentionnées (articles 7, 1° et 3°/1 L.R&S) stipulent que la VSSE a pour (seule et unique) mission – *« de rechercher, d'analyser et de traiter le renseignement »*. Traduites au niveau opérationnel, ces dispositions prévoient que la mission de la VSSE, dans le cadre de son travail de renseignement consiste à mener des enquêtes de renseignement et à transmettre ensuite les résultats de l'enquête à des tiers. L'utilisation ultérieure par la VSSE de ces résultats d'enquête, plus précisément l'utilisation et l'exploitation à des fins d'entrave[34] des renseignements qu'elle produit, n'a aucun fondement dans les dispositions légales susmentionnées.

---

[32] En outre, l'article 13 L.R&S ne peut pas non plus servir de base juridique à cette fin. Il s'agit d'une disposition trop générale pour réglementer la collecte de renseignements dans son ensemble. Tout comme l'article 13 L.R&S, d'ailleurs, est une disposition trop générale pour réglementer la collecte d'informations dans son intégralité. Une position suivie par le législateur à travers l'élaboration des méthodes ordinaires, spécifiques et exceptionnelles (art. 14 à 18/17 L.R&S).

[33] Ou en vertu de toute autre disposition légale réglementant la transmission obligatoire d'informations, comme l'obligation de dénonciation (art. 29 CIC) et l'obligation de communiquer les informations à l'OCAM (art. 6 Loi OCAM).

[34] Une autre finalité est, par exemple, l'utilisation par la VSSE des résultats de ses enquêtes pour orienter les enquêtes de renseignement en cours ou pour en ouvrir de nouvelles.

Les articles 13 à 19 L.R&S (c'est-à-dire les différentes compétences que la VSSE peut utiliser dans le cadre de l'exécution de ses missions de renseignement) ne constituent pas non plus une base pour une mesure de disruption primaire. En effet, ce que fait la VSSE et la manière dont elle le fait sont définis et limités par le motif pour lequel elle le fait (en vertu, entre autres, de l'article 75, 2° de la Loi relative à la protection des données). L'exercice des compétences précitées est donc limité par les finalités énumérées à l'article 7, 1° et 3°/1 L.R&S. En d'autres termes, les compétences visées aux articles 13 à 19 L.R&S doivent être exercées en vue de la collecte, du traitement ou de la transmission d'informations, et non en vue de l'utilisation ultérieure de ces informations par la VSSE.

À titre d'illustration : dans l'état actuel du droit, la VSSE s'est vu confier par le législateur un pouvoir d'observation pour collecter des informations (*cf*. articles 16/1, 18/4 et 18/11 L.R&S), pas pour transmettre un message non verbal et un avertissement à une cible (par le biais d'une observation non discrète, perceptible et visible par cette cible), qu'elle est suivie par la VSSE et ainsi entraver cette personne et ses activités, qualifiées de nuisibles par le service de renseignement.

À titre d''illustration : la VSSE peut *de lege lata* déployer des sources humaines (human intelligence / HUMINT / informateurs) (art. 18 L.R&S). Il s'agit de personnes physiques chargées par le service de renseignement de collecter des informations clandestinement. En l'état actuel de la législation, la VSSE ne peut pas utiliser ces personnes physiques comme agents d'influence, c'est-à-dire des personnes physiques auxquelles le service de renseignement impute l'entrave, secrète ou non, de certaines (qualifiées de menaces par la VSSE). La question de savoir s'ils commettent ou provoquent des infractions pénales en agissant de la sorte est distincte de celle de savoir si les sources humaines gérées par la VSSE peuvent être utilisées comme agents d'influence.

À titre d'illustration : la VSSE est autorisée à signaler les personnes au niveau national et international (par ex. le signalement SIS[35], c'est-à-dire via le système d'information Schengen de l'Union européenne). Ces outils servent à recueillir des informations (par exemple, en cartographiant discrètement les déplacements d'une cible), et non à perturber les activités des individus (par exemple, en contrôlant systématiquement la personne concernée à l'aéroport).

En résumé : **l'utilisation par la VSSE de ses compétences de collecte d'informations (les méthodes de renseignement dites ordinaires, spécifiques et exceptionnelles) dans un but autre que la collecte de renseignements, plus précisément dans l'intention d'utiliser les renseignements avec une finalité d'entrave, viole le principe de limitation de la finalité et le principe de finalité[36] compte tenu de l'énumération actuelle des missions à l'article 7 L.R&S (et de la manière de décrire ces missions utilisée dans le présent document).**

Cependant, la VSSE n'est pas opposée actuellement à un ancrage juridique de la disruption primaire : *« La première étape a consisté à examiner ce qui est possible aujourd'hui dans le cadre légal existant. De là est né le raisonnement concernant les activités d'entrave primaire et secondaire. L'entrave secondaire signifie informer les partenaires afin qu'ils puissent utiliser leur arsenal juridique pour contrer la menace. Les partenaires dans ce contexte sont l'Office des étrangers (accès au territoire) ou les gouverneurs (port d'armes). L'entrave primaire signifie une intervention indépendante par la VSSE (en allant parler à une cible, à son*

[35] Il s'agit de demandes du VSSE au Bureau Sirene belge, créé au sein de la Police fédérale, pour des signalements internationaux via le système d'information Schengen de l'Union européenne.

[36] Également appelé 'principe de spécialité' en droit administratif.

patron…). Des procédures internes ont été établies pour les deux formes d'intervention, qui nous semblent offrir les garanties nécessaires. Nous ne demandons pas de modification de la loi. Cela signifie égalementt que nous ne demandons pas de moyens d'intervention supplémentaires. Nous pensons que pour les prochaines étapes, il est utile d'être obligé de travailler avec des partenaires (entre autres la police et le système judiciaire). C'est ce qui offre le plus de garanties pour un moyen démocratiquement acceptable de contrer les menaces. ».[37]

Comme cela a été mentionné, la Commission d'enquête parlementaire a toutefois estimé qu'il était essentiel, compte tenu de l'impact de l'intervention disruptive sur les droits des personnes ou entités visées, de prévoir les garanties juridiques nécessaires. *« Ces interventions doivent donc se fonder sur une base juridique qui doit encore être créée. Il faudra non seulement y définir les conditions d'application de ces interventions, mais également y prévoir les mécanismes de contrôle nécessaires. »*.[38]

Dans son enquête de contrôle sur le suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes concernant les services de renseignement et de sécurité, le Comité a établi que :

> *« Selon l'interprétation du ministre de la Justice et, par extension, de la VSSE, cette recommandation a été mise en œuvre. Toutefois, le Comité est d'avis que dans un État démocratique et de droit, les activités d'entrave primaire de la VSSE (c'est-à-dire l'intervention d'initiative du service de renseignement dans le cadre d'une activité qu'il a lui-même qualifiée de menace) devraient être réglementées séparément dans une loi suffisamment claire, au sens formel du terme. L'idée sous-jacente est que différents organes doivent être chargés de détecter et d'enquêter sur les éventuelles menaces pour la sécurité nationale, d'évaluer la menace (in casu, il s'agit de déterminer si des individus, des groupes ou des événements constituent effectivement une menace pour la sécurité nationale) et de prendre les mesures nécessaires contre ces menaces. Au minimum, le pouvoir de décision d'intervention doit être entre les mains d'une instance autre que celle qui l'exécute. Une alternative consiste à établir un contrôle externe similaire au contrôle MRD.*
>
> *En effet, les mesures d'entrave primaire à l'encontre d'une personne physique doivent avoir une base juridique du point de vue des droits de l'homme. Le Comité ne partage donc pas l'avis de la VSSE selon lequel aucune intervention juridique n'est nécessaire à cette fin. Toute ingérence dans la vie privée exige une base juridique. Le Comité constate que la VSSE ne demande pas de moyens juridiques supplémentaires (lire: des pouvoir supplémentaires). Les mesures d'entrave primaire – telles que l'avertissement d'un cible (par exemple, un officier de renseignement étranger espionnant sur le territoire belge), à son employeur (par exemple, le service de renseignement étranger), la sensibilisation de ses victimes ou l'entrave à une menace par l'intervention secrète d'une source humaine à la demande d'un service de renseignement –* ***sont autant d'activités qui nécessitent une base juridique en vertu de l'article 22 de la Constitution et de l'article 8.2 de la CEDH****. Le fait que la VSSE ne*

[37] Courrier du Directeur de l'Analyse datée en 3 août 2022 adressée au Président du Comité permanent R concernant les recommandations de la Commission parlementaires Attentats terroristes – réactions de la VSSE. Voir : COMITÉ PERMANENT R, « Enquête de contrôle relative au suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes concernant les services de renseignement et de sécurité », p. 69.

[38] *Doc. parl.,* Chambre , 2016-17, n°54-1752/008, p. 308.

soit pas demandeuse de moyens supplémentaires ne signifie pas qu'une intervention juridique n'est pas nécessaire.[39]
Le Comité constate que, compte tenu de l'objet de l'enquête parlementaire, la commission d'enquête parlementaire s'est limitée à l'entrave dans le cadre de la lutte contre le terrorisme, l'extrémisme et le radicalisme. Ce faisant, le Comité souhaite attirer l'attention sur la (grande) importance d'entrave au sein du contre-espionnage. Il est donc conseillé que l'entrave primaire au sein du contre-espionnage soit également incluse dans un débat parlementaire. ».[40]

Cette évaluation montre déjà clairement que le Comité n'a aucune objection à ce que la VSSE soit dotée d'un pouvoir de disruption primaire. Toutefois, compte tenu de son caractère sensible, elle doit être précédée d'un débat parlementaire, l'objet de la discussion portant sur le contenu de la disruption primaire, les conditions d'application, la procédure à suivre ainsi que le contrôle de l'exercice de ce pouvoir de disruption.

CONCLUSION INTERMÉDIAIRE

En 2017, la Commission d'enquête parlementaire Attentats terroristes a clairement préconisé l'introduction d'un pouvoir de disruption pour la VSSE, et ce tant pour les mesures de disruption primaire que pour les mesures de disruption secondaire. Ce faisant, la Commission d'enquête a insisté – à deux reprises – sur une intervention législative du Parlement. Le Comité note que la VSSE ne demande pas d'élaboration et d'intervention législatives pour la mise en œuvre de sa théorie de la disruption.

En ce qui concerne la disruption secondaire, le Comité estime que le cadre juridique actuel fournit la base. Le Comité recommande toutefois que, comme le prévoit la Loi Renseignement, les conditions et la procédure soient définies plus précisément par le Conseil national de sécurité. À cet égard, le Comité invite à une certaine prudence quant à l'opportunité de classifier une telle directive CNS. Rappelons que la note de service (actualisée) n° 20-29 de la VSSE n'est pas non plus classifiée.[41]

Fondamentalement, une politique de disruption secondaire qui cherche à contrecarrer et à neutraliser délibérément une menace spécifique (par exemple, les activités d'espionnage et d'ingérence d'un pays donné) (par exemple, en entravant certains postes clés au sein de l'appareil de renseignement étranger de ce pays[42]) fait partie intégrante de la mission statutaire de renseignement de la VSSE. D'un point de vue juridique, il s'agit de la communication ciblée d'informations, de conseils avisés et de soutien par la VSSE à d'autres instances (par exemple, le gouvernement et la diplomatie), afin que ces dernières puissent prendre les mesures nécessaires pour contrer les menaces de sécurité pertinentes. **Une politique de disruption secondaire est donc essentiellement une diffusion externe intelligente par la VSSE de ses renseignements, et mérite certainement d'être imitée.**

---

[39] L'article 73 de la loi néerlandaise sur les services de renseignement et de sécurité peut constituer une source d'inspiration.

[40] COMITÉ PERMANENT R, « Enquête de contrôle relative au suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes concernant les services de renseignement et de sécurité », p. 70.

[41] Cette note de service revêt la mention « diffusion restreinte ».

[42] Voir par exemple : Sûreté de l'État, Intelligence report 2021-2022, p. 8 et 9.

Le Comité souhaite faire remarquer que, comme toute politique et comme l'exige l'article 20 § 3 L.R&S, une politique doit être validée par les autorités politiques compétentes (c'est-à-dire le Conseil national de sécurité). En outre, une mesure de perturbation liée à une personne est placée sous le contrôle correctif du Comité permanent R, agissant en tant qu'autorité de protection des données.

En ce qui concerne la disruption primaire, le Comité estime que, tant du point de vue du droit des traités que du point de vue constitutionnel, une intervention législative du Parlement est nécessaire. **Une mesure de disruption liée à une personne doit, en vertu de l'article 22 de la Constitution et de l'article 8.2 de la CEDH, être régie par une loi formelle.** D'un point de vue politique également, un pouvoir de disruption primaire constitue un changement de paradigme trop important dans le domaine du renseignement pour pouvoir se passer d'un débat parlementaire préalable à sa mise en œuvre.

Le Comité recommande plus spécifiquement que, comme dans la législation néerlandaise sur les services de renseignement et de sécurité, la Loi Renseignement ajoute une disposition composée du libellé suivant: *« promouvoir et prendre des mesures pour protéger les intérêts fondamentaux du pays que doit défendre le service et pour combattre les menaces à contenir par le service »*.[43]

Il est important que cette disposition soit ajoutée à l'article 7 L.R&S (c'est-à-dire l'énumération des missions de la VSSE) et ne constitue pas un nouvel article de loi entre les articles 13 à 19 L.R&S (c'est-à-dire l'énumération des pouvoirs dont dispose la VSSE pour accomplir ses missions). L'exigence de légalité énoncée à l'article 22 de la Constitution et à l'article 8.2 de la CEDH est ainsi satisfaite, mais le service est limité dans l'exercice de sa mission de disruption par les moyens / pouvoir dont il dispose déjà (et limité à cet égard par

---

[43] Inspiré de l'article 73 de la Loi néerlandaise relative aux services de renseignement et de sécurité, laquelle stipule que :

"1. De diensten zijn bevoegd tot het bevorderen of treffen van maatregelen ter bescherming van door de desbetreffende dienst te behartigen belangen, al dan niet met behulp van een technisch hulpmiddel.

2. De uitoefening van de bevoegdheid, bedoeld in het eerste lid, is slechts toegestaan, indien Onze betrokken Minister of namens deze het hoofd van een dienst daarvoor toestemming heeft verleend. Het hoofd van een dienst kan aan hem ondergeschikte ambtenaren bij schriftelijk besluit aanwijzen die de toestemming, bedoeld in de eerste volzin, namens hem verlenen. Onze betrokken Minister wordt een afschrift van het besluit, bedoeld in de tweede volzin, gezonden.

3. Bij het bevorderen of treffen van een maatregel wordt slechts die maatregel bevorderd of getroffen, die gelet op de omstandigheden van het geval, waaronder de ernst van de bedreiging van de door een dienst te beschermen belangen, voor de betrokkene het minste nadeel oplevert. Artikel 26, tweede tot en met vierde lid, is van overeenkomstige toepassing."

➔ Traduit dans la Loi Renseignement, il s'agit des exigences de subsidiarité et de proportionnalité.

"4. Het bevorderen of treffen van maatregelen als bedoeld in het eerste lid kan bij een instructie als bedoeld in artikel 41, eerste lid, worden opgedragen aan een natuurlijke persoon als bedoeld in dat artikel."

➔ Traduit dans la Loi Renseignement, il s'agit d'une source humaine.

"5. In het geval dat het bevorderen of treffen van maatregelen wordt opgedragen aan een medewerker van de dienst, is artikel 41, vierde tot en met zevende lid, van overeenkomstige toepassing, met dien verstande dat onder «de natuurlijke persoon» of «persoon» in de desbetreffende artikelleden wordt verstaan: de medewerker van de dienst die wordt belast met de feitelijke uitvoering van de in het eerste lid bedoelde handelingen."

➔ Traduit dans la Loi Renseignement, il s'agit (1) de la commission d'infractions par un agent de la VSSE, (2) de l'interdiction d'incitation à la commission d'une infraction, (3) des conditions matérielles et formelles pour la commission d'une infraction.

l'exigence de légalité visée à l'article 12 L.R&S[44]). Il convient de débattre séparément de la question de savoir quelles compétences supplémentaires la VSSE doit obtenir, le cas échéant, à cet égard (*infra*). Le Comité estime cependant que le service de renseignement ne doit pas se voir attribuer le pouvoir spécifique de faire usage de la force.[45] Selon le Comité, la VSSE n'est pas un service de police et ne peut pas non plus le devenir.[46] Il ressort clairement d'une correspondance antérieure de la VSSE que le service n'est pas non plus demandeur.[47] L'incitation à la commission d'infractions doit également demeurer interdite, comme c'est le cas actuellement. Un agent d'influence ne peut être autorisé à provoquer des infractions.

Il est significatif qu'ici, comme aux Pays-Bas, une exigence de subsidiarité et de proportionnalité soit également insérée dans la loi. Le Comité laisse ouverte la question de savoir si, dans le cadre de la mise en œuvre d'une mesure de disruption primaire, comme c'est le cas dans la réglementation néerlandaise, la VSSE doit pouvoir utiliser une source humaine (*supra*, un agent d'influence), un moyen technique et un agent de la VSSE pouvant commettre des infractions.

Enfin, le Comité préconise que sa mise en œuvre implique un contrôle externe similaire au contrôle MRD, le contrôle MPLUS[48] (avec notification obligatoire *ex officio* au Comité) ou au contrôle DPA du Comité. Dans ce cadre, le Comité exercera un contrôle et aura le pouvoir de prendre des mesures correctrices en cas d'illégalité identifiée.

---

[44] Article 12 L.R&S : *« Pour accomplir leurs missions, les services de renseignement et de sécurité ne peuvent utiliser des moyens de contrainte que dans les conditions prévues par la loi. »*.

[45] Au sein de la VSSE, une 'Incident Response Team' (ce que l'on appelle l'équique d'intervention *cf.* art. 22 L.R&S) dispose cependant du pouvoir de faire usage de la force. Pour plus d'informations à ce propos : VERSCHAEVE, B., "Het Incident Response Team van de Staatsveiligheid. De interne beveiligingsdienst van de burgerlijke inlichtingendienst toegelicht", *Politie en Recht* nr. 1/2022, p. 3-20.

[46] Les agents de la VSSE peuvent exceptionnellement – comme tout citoyen d'ailleurs – appliquer la force (proportionnelle) et même brièvement (en attendant l'arrivée de la police) priver une personne de sa liberté dans le cadre d'une défense légitime (article 416 CP). De plus, dans ce contexte, la récente décision du ministre de la Justice selon laquelle les agents de la VSSE autres que les opérateurs IRT disposent d'une arme de poing mais ne disposent plus de menottes dans le cadre de leur équipement réglementaire pose question. En effet, un usage proportionné de la force dans l'exercice d'une défense légitime exige que, dans certains cas, les agents de la VSSE disposent de menottes. Si, dans une situation d'intervention d'urgence, un agent de la VSSE ne porte qu'une arme de poing (par exemple lors d'une observation) alors qu'un agresseur doit être tenu en joue mais où la simple menace de tirer n'est plus efficace, alors le tir réel est la seule alternative si cet agent de la VSSE ne dispose pas de menottes pour immobiliser l'agresseur (jusqu'à l'arrivée de la police). L'absence de menottes (les menottes classiques en métal ou les menottes en plastique dont l'utilisation est autorisée) dans une telle situation conduit toujours à un usage disproportionné de la force. Voir l'article 3 de l'Arrêté ministériel du 16 juin 2022 déterminant l'équipement réglementaire des agents de la Sûreté de l'État et fixant les dispositions particulières relatives à la détention, au port et à la garde de l'armement (*M.B.* 19 octobre 2022).

[47] Lettre datée du 3 août 2022 du Directeur de l'Analyse au Président du Comité permanent R concernant les recommandations de la commission d'enquête parmentaire Attentats terroristes – réactions VSSE. Voir COMITÉ PERMANENT R, « Enquête de contrôle relative au suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes concernant les services de renseignement et de sécurité »,
p. 69.

[48] Il s'agit des méthodes de renseignement ordinaires des articles 16/2 à 16/4 L.R&S, qui élaborent un mécanisme de contrôle particulier.

1.2.3 Différentes sortes de mesures de disruption

Une annexe classifiée intitulée « Boîte à outils entrave VSSE » (également appellée 'disruption toolkit') accompagne la note de service n° 18-50 du 5 novembre 2018. Cette boîte à outils contient une énumération des mesures de disruption primaire et secondaire. Bien que la note de service en question ait depuis été remplacée par la note de service n° 20-29 du 11 juin 2020, la boîte à outils reste valable. La note de service n° 18-50 établit à ce propos : *« Les collègues qui envisagent une entrave peuvent s'inspirer de la boîte à outils 'entrave' […]. Il est possible de mettre en oeuvre une ou plusieurs mesures d'entrave, tout comme il peut être envisagé de combiner des mesures primaires et secondaires. »*.[49]

Tant la note de service n° 18-50 que la note de service actualisée imposent l'utilisation d'un document standard / modèle pour la procédure d'entrave primaire. Ce formulaire circonstanciel contient l'évaluation et la motivation d'une proposition de disruption primaire (c'est-à-dire la justification de l'entrave, les objectifs visés, la description de la mesure envisagée, l'évaluation de différents types de risques, notamment de nature opérationnelle, juridique, diplomatique, organisationnelle et sécuritaire, le point de vue des gestionnaires de dossier concernés, la décision de la ligne hiérarchique, ainsi que la décision finale de l'Administrateur général. Comme le prévoient déjà les notes de service n°18-50 et n°20-29, la 'Boîte à outils entrave VSSE' est avant tout une source d'inspiration. Le choix final de la mesure envisagée est déterminé et décrit dans le formulaire d'entrave. **Le Comité se félicite certainement de l'exitence et du contenu de ce formulaire.** Toutefois, il est indiqué d'y apporter une modification mineure mettant davantage l'accent sur les exigences de subsidiarité et de proportionnalité. Le Comité recommande que dans le cadre de son contrôle prospectif et plus détaillé, ce formulaire soit utilisé comme point de départ du contrôle externe.

Cependant, l'absence d'une liste exhaustive de mesures de disruption primaire, validée par le Conseil national de sécurité, fondée sur des principes généraux et des limites fixées par une assemblée législative démocratiquement élue, soulève, en l'état actuel des choses, des questions sur la légalité et la légitimité démocratique de la mise en œuvre de la théorie de la disruption (primaire) par la VSSE. Il ne saurait être question pour la VSSE de décider elle-même des moyens d'action dont elle dispose pour perturber les activités qu'elle qualifie de menaces par elle-même (c'est-à-dire par des mesures de disruption primaire). Il reste en outre à voir si la VSSE est demandeuse, en gardant à l'esprit sa quête permanente, au fil des ans, de faire approuver des points importants (par exemple la définition de ses priorités) par le Conseil national de sécurité.

1.3 CONDITIONS D'APPLICATION

1.3.1 Actuellement

Dans les notes de service n° 18-50 et 20-29, la VSSE établit que : *« (l') entrave est la pertubation des menaces de sorte qu'elles ne se produisent plus ou d'en réduite*

[49] Note de service n° 18-50, p. 2.

considérablement la nocivité. ». La Commission d'enquête parlementaire[50], citant[51] textuellement la définition de la VSSE déclare que : *« La commission d'enquête […] estime qu'il convient de permettre à la VSSE de perturber suffisamment certaines activités nuisibles pour qu'elles n'aient plus lieu, ou du moins pour réduire leur nocivité. Il s'agirait de perturbations visant non seulement des personnes, mais aussi d'autres entités, par exemple une librairie radicale ou un établissement d'enseignement radical. »*.

Dans la note de service n° 18-50, la VSSE examine plus en détail les conditions préalables qui peuvent être réunies pour pouvoir procéder à une entrave. Il est prévu que *« [l'] entrave peut être envisagée dans un dossier et/ou sur une target au moment où, par exemple :*

- *La menace est importante et le risque n'est plus contrôlé,*
- *La simple collecte de renseignements et la mise en oeuvre de méthodes de renseignement n'ont plus de sens,*
- *Certains événements survenant dans le dossier offrent une opportunité d'entrave,*
- *Une menace identifiée qui n'est pas assez importante pour justifier d'investir plus avant des moyens humains et métériels mais ont le dossier offre par contre des possibilités d'entrave,*
- *La nature de la menace oblige la VSSE à impliquer des partenaires externes dans l'entrave,*
- *Les objectifs initiaux sont atteints dans un dossier et celui-ci peut être clôturé. »*.[52]

La note de service n° 20-29, qui abroge et remplace la note de service n° 18-50, ne reprend pas ce passage et n'établit pas de nouvelles conditions matérielles.

1.3.2 Les perspectives

Les règlements internes actuels n'accordent que peu ou pas d'attention aux conditions matérielles qui doivent être réunies *a priori*, avant de procéder à une disruption. Les agents de la VSSE qui souhaitent procéder à la disruption d'un cas donné doivent fournir les justifications requises. Mais cette obligation ne change logiquement rien au fait qu'il n'existe pas de conditions générales d'application au sein du service de renseignement, c'est-à-dire des conditions qui doivent être présentes de manière générale (lire : dans tous les dossiers) lors de la prise d'une mesure de disruption primaire et / ou secondaire. Dans la note de service n° 18-50, une plus grande attention a été accordée à ce point. Le Comité constate que les conditions concernées ne sont / n'étaient pas exhaustives, incohérentes et inapplicables. Cette disposition a été supprimée dans la note de service n° 20-29.

Le Comité recommande que le législateur (en ce qui concerne la disruption primaire) et le Conseil national de sécurité (en ce qui concerne la disruption secondaire) définissent les conditions d'application pour procéder à l'entrave. Le Comité tient à souligner ici que, du point de vue des droits fondamentaux et des droits de l'homme, il n'est en aucun cas possible qu'une telle disposition soit classifiée (intégralement) dans une directive CNS.

---

50 *Doc. parl.*, Chambre, 2015-2016, n° 54-1752/008, p. 56 et 308.

51 Note du 31 août 2016 de l'Administateur général de la VSSE au Président de la Commission d'enquêtes Attentats, aux ministres de la Justice et de l'Intérieur et au Président du Comité permanent R, p. 24 (concernant le projet de disprution).

52 Note de service n° 18-50, p. 2.

1.4 PROCÉDURES

1.4.1 Actuellement

La note de service n° 20-29, outre un rappel de la définition de la disruption employée par la VSSE, traite exclusivement des procédures / processus de travail internes sur la disruption primaire et secondaire.

Concertation et accord entre partenaires internes

« La première étape dans la procédure consiste en une concertation et à l'atteinte d'un accord entre les partenaires internes qui sont impliqués dans le dossier (service d'analyse et service extérieur) et les partenaires internes dont la présence est nécessaire afin d'exécuter l'entrave (par exemple, officier de liaison, Humint,…). Le gestionnaire du dossier, le OWNER du dossier, organise une concertation.

Les sujets de discussion lors de la concertation porteront sur l'opportunité d'une entrave, la faisabilité des mesures choisies, l'acceptation des risques éventuels et la disponibilité du personnel pour une mise en oeuvre optimale de l'entrave.

En cas de disruption primaire, la présence de JUR[53] est nécessaire. JUR procédera à l'évaluation juridique des mesures d'entraves primaires.

Dans le cas d'une combinaison de mesures primaires et secondaires, la procédure disruption primaire doit être suivie. ».

Procédure entrave primaire

La note de service énumère ensuite les phases successives :

- Le gestionnnaire du dossier effectue les travaux préparatoires nécessaires, notamment l'enregistrement dans la base de données de la VSSE et le remplissage du formulaire d'entrave sur la base des décisions prises lors de la concertation préliminaire ;
- Le formulaire d'entrave suit la voie hiérarchique ;
- La direction de la VSSE discute du dossier d'entrave ;
- Le dirigeant de la VSSE prend la décision finale (mise en oeuvre ou non de la disruption).

Procédure entrave secondaire

« Concernant les entraves secondaires, la procédure actuelle reste inchangée. La demande, par le biais de NE ou de NA aux partenaires externes, suit la voie hiérarchique. ». Comme mentionné, la mise en œuvre d'une mesure de disruption secondaire se fait par le biais d''une note à une instance (publique) belge (NA) et ou par la biais d'une note à un service de renseignement et de sécurité étranger (NE).

[53] Le service juridique de la VSSE.

La VSSE veille également à fournir des informations contextuelles à l'instance (publique) belge et / ou au service de renseignement et de sécurité étranger concerné : la note de service précise que *« [u]ne communication interne claire, ouverte et complète avec le LO (qui entretient la relation avec le partenaire externe concerné) au sujet de l'objectif stratégique de l'entrave, incluant éventuellement des scénarios alternatifs, aide à prévenir des malentendus. »*.

1.4.2 Les perspectives

Les règlements internes actuels traitent de manière adéquate les procédures internes à suivre avant de procéder à une disruption.

Cependant, le Comité recommande que le législateur (en ce qui concerne la perturbation primaire) et le Conseil national de sécurité (en ce qui concerne la perturbation secondaire) définissent le pouvoir de décision pour procéder à la disruption.

Pour la disruption primaire, le Comité estime qu'il devrait s'agir de l'Administrateur général (adjoint), sans possibilité de délégation (*cf.* procédure MRD)

Pour la disruption secondaire, le Comité est d'avis qu'il devrait s'agir de l'Administrateur général (adjoint), mais avec une possibilité de délégation. Le Comité recommande fortement de limiter l'option de délégation au niveau du directeur, soit le niveau juste en dessous de l'Administrateur général adjoint de la VSSE. Compte tenu du degré d'interférence avec la vie privée, il n'est pas défendable qu'un pouvoir de disruption puisse être délégué à un niveau inférieur.

Enfin, le Comité recommande la création d'une obligation de notification dans la Loi Renseignement, imposant aux services de renseignement et de sécurité d'informer les autorités de sécurité (par ex. l'ANS en ce qui concerne les habilitations, attestations et avis de sécurité) des menaces de sécurité qu'ils ont détectées dans le cadre de leur mission de renseignement, lorsque la personne fait l'objet d'un screening de sécurité.

1.5 MANDATAIRES POLITIQUES[54]

Il convient d'accorder une attention particulière aux passages de la note de service n° 20-29 traitant des entraves en cas d'implication d'un mandataire politique.

Il y est stipulé que : *« (l)orsqu'un mandataire politique est concerné par une entrave primaire[55], le OWNER[56] doit cocher la case mandataire politique dans le document « modèle 90 »[57] et rédige également une NA pour le ministre de tutelle et le Premier Ministre. Une copie de cette NA sera également destinée au président du Comité R. […] AG[58] sera personnellement informé de l'approche et du timing, si un entretien direct avec un mandataire politique fait*

[54] Le Comité a déjà effectué plusieurs enquêtes de contrôle sur le 'Suivi des mandataires politiques'. Voir COMITÉ PERMANENT R, *Rapport d'activités 1998*, p. 65 et suiv., *Rapport d'activités 1999*, p. 13 et suiv., *Rapport d'activités 2008,* p. 25 et suiv., *Rapport d'activités 2013*, p. 37 et suiv. et *Rapport d'activités 2021*, p. 30 et suiv.

[55] Souligné par le Comité permanent R.

[56] Le gestionnaire de dossier.

[57] Le formulaire d'entrave.

[58] L'Administrateur général de la VSSE.

partie de la disruption. ».[59] En ce qui concerne la disruption secondaire, il est mentionné que: *« (l)orsqu'un mandataire politique est concerné par une entrave secondaire, le OWNER rédige une NA […]. »*.

Dans son Rapport d'activités 2021, le Comité écrit ce qui suit :
« Lors de débats (parlementaires), une question est posée à maintes reprises, à savoir si et dans quelle mesure les services de renseignement belges suivent (ou sont autorisés à suivre) des mandataires politiques, et quelles règles doivent être observées à cet égard. Depuis début janvier 2018, une note de service classifiée 'CONFIDENTIEL' est d'application au sein de la VSSE. Conformément à cette note, actualisée en juin 2020 [60], le service envoie deux types de rapports au ministre de la Justice et au Premier ministre, avec copie au Comité permanent R. Il s'agit, d'une part, de rapports ponctuels sur des mandataires politiques qui contribueraient à l'apparition d'une menace et, d'autre part, d'un aperçu trimestriel de l'ensemble des documents dans lesquels des mandataires politiques sont mentionnés.
Le ministre de la Justice avait marqué son accord sur le 'principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991'.[61]
Étant donné qu'il n'est mentionné nulle part ce que le Comité permanent R est censé faire des informations précitées, il a pris l'initiative de développer une méthodologie autour de cette problématique et de son rôle de contrôle. Cette méthodologie a été approuvée par la Commission parlementaire de suivi en 2020. ».[62]

Les mandataires politiques visés sont les ministres des différents gouvernements, le Commissaire belge siégeant à la Commission européenne et les membres des différents parlements et assemblées, y compris les membres belges du Parlement européen. Les autres élus ou mandataires désignés ne sont pas concernés (par ex. les échevins au niveau communal ou les gouverneurs au niveau provincial).[63]

En ce qui concerne la problématique de la disruption dans le cas où un mandataire politique est impliqué, la note de service n° 20-29 doit être lue conjointement avec la note de service de la VSSE n° 20-28.[64] Cette dernière note de service réglemente la manière dont le personnel de la VSSE doit traiter le cas où certains mandats politiques apparaissent dans les documents de la VSSE.

Celle-ci établit que : *« (i)l n'est jamais exclu que des madataires politiques apparaissent dans les informations recueillies par la VSSE (dans le cadre de l'exercice de leur mandat/en marge d'une menace). Ils peuvent être cités par des sources humaines, mentionnés dans des messages des services homologues, dans des articles de presse, repris dans des listes établies suite à la mise en œuvre de moyens techniques (par ex. des listes de numéros de téléphone).*

---

59 Note de service n° 20-29, p. 2-3.
60 Cette note de service actualisée n'est pas classifiée, contrairemement à la note de service précédente.
61 Voir le courrier du ministre de la Justice daté du 26 juillet 2018 et adressé au Comité permanent R sur 'le recueil d'informations par un service de renseignement concernant une personne exerçant un mandat politique', mentionné dans COMITÉ PERMANENT R, *Rapport d'activités 2021*, p. 31, note de bas de page 61.
62 COMITÉ PERMANENT R, *Rapport d'activités 2021*, p. 30-32.
63 Note de service n° 20-28, p. 2.
64 Note de service n° 20-28 du 11 juin 2020 de l'Administrateur général de la VSSE concernant les mandataires politiques (diffusion restreinte).

Dans de tels cas, les responsables politiques n'apparaissent que fortuitement dans le champ du service de renseignement. ».[65]

Et indique en outre que : *« Dans le cadre de son fonctionnement opérationnel, la VSSE ne réserve pas aux mandataires politiques un traitement différent de celui accordé aux autres catégories professionnelles. S'il existe des raisons d'examiner de plus près l'éventuelle implication d'un mandataire politique dans la survenue d'une menace, il convient de le faire. Sauf bien sûr dans les cas où le mandataire politique est impliqué en tant que victime dans la survenue d'une menace. Toutefois, lorsque des mandataires politiques sont concernés, un certain nombre de mécanismes doivent être appliqués afin d'éviter tout abus de position de la part du service. Parmi ces mécanismes figure notamment le devoir d'information aux ministres compétents dès qu'il y a présomption d'implication d'un mandataire politique dans la survenue d'une menace. ».*[66]

La règle suivante présente un intérêt immédiat pour cette analyse juridique :

« Dès que les informations disponibles permettent d'établir l'implication d'un mandataire politique dans la survenue d'une menace, la Direction générale est informée par le biais d'un rapport interne. Ensuite, après approbation de la Direction générale, le ministre de la Justice et le Premier ministre doivent en être informés par le biais d'une NA (en copie au Comité R). A cet égard, il convient de ne prendre en compte que les informations confirmées ou considérées comme très probables et qui ont été analysées et vérifiées.

La NA doit comporter au minimum les éléments suivants :

- *Une description de la façon dont le mandataire politique contribue à la survenue de la menace.*
- *Une estimation des éventuelles conséquences que cette implication peut engendrer ou a engendré.*
- *Quel sera le suivi ultérieur du dossier par la VSSE.*
- *Les mesures qui seront prises par le service dans ce cas concret (par ex. informer les autorités judiciaires / informer le Président du Parlement / informer le ministre-Président / entretien avec le mandataire concerné / …). S'il devait y avoir des mesures d'entrave, la note de service DNS 20-29 doit être suivie.*[67]
- *Si nécessaire, il y a lieu de formuler des recommandations à l'attention du ministre de la Justice et du Premier ministre. ».*[68]

Il ressort clairement des notes de service n° 20-28 et n° 20-29 que la VSSE s'estime compétente pour prendre des mesures perturbatrices à l'encontre des activités des parlementaires fédéraux et régionaux et des ministres qualifiés de problématiques, et manifestement tant pour des disruptions secondaires (c'est-à-dire informer et conseiller les autorités compétentes) que pour des disruptions primaires (c'est-à-dire prendre elle-même des mesures d'exécution).

Compte tenu de l'importance de la présente problématique, le Comité souhaite tout d'abord rappeler les recommandations émises dans l'enquête de contrôle relative au suivi des

[65] Note de service n° 20-28, p. 4.
[66] Note de service n° 20-28, p. 4 et 5.
[67] Souligné par le Comité permanent R.
[68] Note de service n° 20-28, p. 6-7.

recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes :

> *« […] le Comité est d'avis que dans un État démocratique et de droit, les activités d'entrave primaire de la VSSE (c'est-à-dire l'intervention d'initiative du service de renseignement dans le cadre d'une activité qu'il a lui-même qualifiée de menace) devraient être réglementées séparément dans une loi suffisamment claire, au sens formel du terme. L'idée sous-jacente est que différents organes doivent être chargés de détecter et d'enquêter sur les éventuelles menaces pour la sécurité nationale, d'évaluer la menace (in casu, il s'agit de déterminer si des individus, des groupes ou des événements constituent effectivement une menace pour la sécurité nationale) et de prendre les mesures nécessaires contre ces menaces. Au minimum, le pouvoir de décision d'intervention doit être entre les mains d'une instance autre que celle qui l'exécute. Une alternative consiste à établir un contrôle externe similaire au contrôle MRD.*
>
> *En effet, les mesures d'entrave primaire à l'encontre d'une personne physique doivent avoir une base juridique du point de vue des droits de l'homme. Le Comité ne partage donc pas l'avis de la VSSE selon lequel aucune intervention juridique n'est nécessaire à cette fin. Toute ingérence dans la vie privée exige une base juridique. […] ».*[69]

Deuxièmement, le Comité souhaite rappeler **que dans l'application de la disruption primaire – en l'absence de cadre juridique – la VSSE détermine elle-même quand une activité doit être considérée comme une menace pour la sécurité de l'État, que le service de renseignement détermine lui-même quand une mesure de disruption primaire doit être déployée, qu'il détermine quelle mesure il va déployer, et qu'il n'existe pas de conditions générales d'application.**

Si le Comité considère que cette conclusion de l'analyse ci-dessus est problématique pour les cibles « ordinaires », elle est au moins aussi vraie lorsqu'il s'agit de prendre et de mettre en œuvre des mesures de perturbation primaire contre des titulaires de mandats politiques désignés.

Troisièmement, la question se pose de savoir sur la base de quel critère la VSSE a interprété la notion de « mandataire politique ». Actuellement, la VSSE considère comme « mandataires politiques » les ministres des différents gouvernements, le commissaire belge à la Commission européenne et les membres des différents Parlements. Le Comité estime que par souci d'objectivité, il conviendrait d'inclure toutes les personnes couvertes par l'application de l'obligation de déclaration des mandats à la Cour des comptes, telle que stipulée dans les Lois du 2 mai 1995.

[69] COMITÉ PERMANENT R, « Enquête de contrôle relative au suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes concernant les services de renseignement et de sécurité », p. 69.

PARTIE II. ENTRAVE PAR LE SGRS

2.1 GÉNÉRALITÉS

La théorie de la disruption a été créée par la VSSE à la suite des travaux et des auditions de la Commission d'enquête parlementaire Attentats terroristes. La question est soulevée pour la première fois dans une note de la VSSE adressée au Président de la Commission d'enquête parlementaire.

Il n'existe pas de théorie générale de la perturbation au sein du SGRS. La théorie de la disruption ou un concept similaire n'a été évoqué ni dans la note du 2 septembre 2016 du Chef du SGRS adressée au Président de la Commission d'enquête parlementaire[70] Attentats terroristes, ni lors de son audition le 5 octobre 2016 devant cette commission.[71] La Commission d'enquête parlementaire n'a pas non plus formulé de recommandation à l'intention du SGRS concernant la problématique de la disruption.

Ceci est surprenant. Si l'analyse ci-dessus montre qu'il reste encore beaucoup à faire en termes d'élaboration juridique – notamment en ce qui concerne la protection juridique des citoyens – le concept politique et opérationnel de la disruption est louable. **L'idée selon laquelle un service de renseignement doit se comporter de manière plus active dans la lutte contre les activités qui menacent la sécurité de l'État mérite d'être développée également au sein du renseignement militaire.** D'ailleurs, la Commission d'enquête parlementaire elle-même l'exprime très précisément en déclarant que *« [l]a Belgique part généralement du principe que les services de renseignement jouent essentiellement un rôle d'information qui se traduit par la transmission de renseignements aux autres services publics. La commission d'enquête estime qu'il conviendrait de confier des responsabilités plus étendues à la VSSE dans le domaine de la lutte contre la radicalisation, de l'extrémisme et du terrorisme. Sur ce point, la commission d'enquête se rallie à la théorie de la disruption proposée par l'administateur général de la VSSE. Elle estime qu'il convient effectivement de permettre à la VSSE de perturber suffisamment certaines activités nuisibles pour qu'elles n'aient plus lieu, ou du moins pour réduire leur nocivité. »*.[72] **Le Comité estime que cette recommandation, notamment en ce qui concerne la disruption secondaire, doit également s'appliquer au SGRS.**

Il convient cependant d'ajouter un élément important : malgré le fait qu'il n'existe pas de théorie générale de la disruption au sein du SGRS, il existe une disruption au sein du service dans certaines matières spécifiques. De plus, contrairement à la VSSE, le législateur a abordé cette question dans le passé dans le cadre des activités du SGRS. Tant dans les dispositions

---

70 Cette note du SGRS datée du 2 septembre 2016 est également destinée au ministre de la Défense, au Chef de la Défense et au Comité permanent R.

71 Annexe n°1 du Troisième Rapport intermédiaire sur le volet "architecture de la sécurité" fait au nom de la Commission d'enquête parlementaire (…) – Rapports intégraux des réunions publiques, *Doc. parl,*. Chambre, 2015-2016, n° 54-1752/008, p. 78-100.

72 Troisième Rapport intermédiaire sur le volet "architecture de la sécurité" fait au nom de la Commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste, *Doc. parl.*, Chambre, 2015-2016, n° 54-1752/008, p. 308-309.

légales énumérant les missions du SGRS (notamment l'art. 11 L.R&S) que dans les dispositions réglementant certaines compétences cyber du SGRS (notamment l'art. 44/1 L.R&S), il existe des instruments qui peuvent être joints à une théorie de la disruption du SGRS. Ainsi, bien qu'il n'existe pas de théorie générale de la disruption au sein du SGRS, il peut être établi que que dans le cadre juridique du service de renseignement militaire, il existe déjà une (ébauche d') élaboration juridique pour certaines formes de disruption.

2.2 CADRE LÉGAL

Nous nous référons ici aux sections suivantes de la Loi Renseignement:

L'article 11, § 1er, 1° L.R&S, qui reprend **la mission de renseignement du SGRS**, stipule que le service est chargé de mener des enquêtes de renseignement sur certains événements et menaces ainsi que de *« d'en informer sans délai les ministres compétents ainsi que **de donner des avis** au gouvernement, à la demande de celui-ci, concernant la définition de sa politique extérieure de défense »*. Ce genre d'avis est parfaitement conforme à la proposition de l'Administrateur général de la VSSE à la Commission d'enquête parlementaire : "*Als wij tot nu toe onze rol vaak beperkten tot het louter informeren van de autoriteiten, dan denk ik dat wij nu actiever moeten proberen te communiceren inzake de inlichtingen die door onze dienst kunnen worden verstrekt. Eventueel kunnen die vergezeld gaan van een soort van beleidsadvies, waarbij wij bepaalde zaken aanraden om te doen."*.[73] [74] En outre, il convient de noter que l'article 11, § 1er, 1° L.R&S se situe plutôt au niveau des conseils formulés dans le cadre de l'élaboration d'orientations stratégiques[75], alors que l'Administrateur général du VSSE fait également et plutôt référence à la proposition intentionnelle aux destinataires de ses renseignements de prendre certaines mesures dans des cas individuels concrets (par exemple, le retrait du permis de séjour d'un étranger agissant sur le territoire belge en tant qu'agent d'un service de renseignement étranger).

L'article 11, § 1er, 2° et 2°/1 L.R&S contient **la mission de cybersécurité du SGRS.** Dans ce cadre, le renseignement militaire est chargé, entre autres, de neutraliser une cyberattaque contre certains systèmes informatiques et de communications *« et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par **une propre cyberattaque**, dans le respect des dispositions du droit international »*.[76]

---

[73] Audition du 5 octobre 2016 de l'Administrateur général de la VSSE, *Doc. parl.,* Chambre, 2015-2016, n° 54-1752/008, p. 118.

[74] *« Si jusqu'à présent nous avons souvent limité notre rôle à la simple information des autorités, je pense que nous devrions maintenant essayer de communiquer plus activement sur les renseignements que peut fournir notre service. Ils pourraient éventuellement être accompagnés d'une sorte de conseil politique, dans lequel nous recommandons certaines choses à faire. »* (traduction libre).

[75] Voir également *Doc. parl.,* Chambre 2015-2016, n° 54-2043/001, 8, p. 32-33.

[76] Pour information : K. CLERIX, "Knack duikt in de digitale loopgraven: wat doet het nieuwe Cyber Command van het Belgische leger?", *Knack* 17 octobre 2022; J. MATRICHE, "Cyberespace, le nouveau champ de bataille de l'armée belge", *Le Soir* 18 octobre 2022; "Defensie houdt Cybercommando boven het doopvont", *Belga* et *De Morgen* 18 octobre 2022; P. DE LOBEL, "Cyber Command moet beschermen én vechten", *De Standaard* 20 octobre 2022; J. VAN HORENBEEK, "Hoofd nieuwe Cyber Command: 'We zullen te werk gaan zoals een sluipschutter. Kijken, wachten en indien nodig toeslaan'.", *De Morgen* 20 octobre 2022.

Enfin, l'article 44/1 L.R&S dispose que le SGRS *« peut procéder à l'intrusion dans un système informatique situé à l'étranger, y lever toute protection, y installer des dispositifs techniques en vue du décryptage, du décodage, du stockage et* ***de la manipulation des données stockées, traitées ou transmises par le système****, et* ***perturber et neutraliser le système informatique*** *[…] »*. La VSSE peut elle aussi accéder aux systèmes informatiques (*cf*. art. 18/16 L.R&S). Cette compétence concerne toutefois une méthode (exceptionnelle) de recueil de données. Sur la base de ce texte, la VSSE (et le SGRS pour les systèmes informatiques qui ne sont pas situés à l'étranger) ne peut manipuler les données numériques de quelque manière que ce soit, ni perturber et neutraliser les systèmes informatiques. Ceci est même expressément interdit par la loi.[77]

Comme faisant partie intégrante des Forces armées, il est important de noter que, outre la Loi Renseignement, les activités du SGRS sont également en partie réglementées par la Loi du 20 mai 1994 relative à la mise en oeuvre des forces armées, à la mise en condition, ainsi qu'aux périodes et positions dans lesquelles le militaire peut se trouver et par ses arrêtés d'exécution. Dans ce cas, le SGRS agit en tant que tel comme un service d'action militaire. Étant donné que le Comité permanent R a la mission légale de contrôler le SGRS et toutes ses activités, il a été chargé par le législateur de contrôler le SGRS au cas où celui-ci prendrait des mesures d'entrave.

2.3 CYBER

La mission de cybersécurité est exercée par la composante Cyber Command du SGRS. Créée en octobre 2022, cette structure succède à la Direction Cyber du SGRS. Elle est dirigée par un général-major (le 'Cyber Commander').

À propos de la mise en place de cette nouvelle composante, le nouveau Cyber commander a déclaré dans les médias :

> "*We zijn een onderdeel van de militaire inlichtingendienst ADIV. We worden gecontroleerd door het Comité I en de commissie Landsverdediging.*".[78] [79]

L'opérationnalisation de la mission de cybersécurité a donc lieu par le biais d'une cybercapacité militaire distincte et se concrétise par les fonctionnalités suivantes :

- *cyberdefense* (cybercapacités défensives)
- *cyberintelligence* (travail de renseignement dans le monde virtuel)
- *cyberoperations* (cybercapacités offensives)

En ce qui concerne plus spéciquement les cybercapacités offensives, le Cyber commander a déclaré ce qui suit :

---

[77] Article 18/16, alinéa 3 L.R&S : *« L'intrusion des services de renseignement et de sécurité dans les systèmes informatiques, visée à l'alinéa 1er, ne peut avoir d'autre but que le recueil de données pertinentes qui y sont stockées, traitées ou transmises, sans qu'il y ait destruction ou altération irréversible de celles-ci. »*.

[78] K. CLERIX, "België maakt zich klaar voor de cyberoorlog. Op bezoek bij het nieuwe Cyber Command", *Knack* 19 octobre 2022, p. 39.

[79] *« Nous faisons partie du service de renseignement militaire SGRS. Nous sommes contrôlés par le Comité R et la Commission de la Défense nationale »* (traduction libre).

> *"Vergelijk het met een scherpschutter. 99 procent van de tijd zit je verborgen om een legitiem doelwit te volgen, slechts 1 procent van de tijd zul je schieten. Met zo min mogelijk colleterale schade. Vertaald naar de cyberwereld: zodra je binnen raakt in een netwerk, camoufleer je je en wacht je. Tot je op een gegeven moment in actie komt en een onderdeel van het netwerk tijdelijk neutraliseert. Als je tegenstrever het netwerk gebruikt om tanks te vervoeren van punt A naar punt B bijvoorbeeld."*.[80] [81]

Pour une interprétation et une opérationnalisation concrètes de la mission de cybersécurité du SGRS, il convient d'utiliser, entre autres, le 'Glossary of terms and definitions' du NATO Standardization Office (NSO). La (dernière) édition 2021 introduit plusieurs nouveaux termes cyber, notamment la notion de 'offensive cyberspace operation' / 'opération cybernétique offensive' (en abrégé : OCO): *"Actions in or through cyberspace that create effects to achieve military objectives."*.[82]

PARTIE III. CONCLUSIONS ET RECOMMANDATIONS

À la lumière de la présente analyse juridique, le Comité souhaite formuler les recommandations suivantes :

EN CE QUI CONCERNE LA DISRUPTION SECONDAIRE

- Pour mettre en œuvre la recommandation relative à la disruption formulée par la Commission d'enquête parlementaire Attentats terroristes, l'adoption d'**une Directive du Conseil national de sécurité** (*cf.* art. 20, § 3 L.R&S) définissant les conditions de fond et de forme dans lesquelles la VSSE et le SGRS peuvent procéder à l'adoption et à la mise en œuvre de mesures de **disruption** secondaire (pour la transmission de renseignements tant au niveau national qu'international).
- La création d'une obligation légale de notification, imposant à la VSSE et au SGRS d'informer les autorités de sécurité (par ex. l'ANS en ce qui concerne les habilitations, attestations et avis de sécurité) des menaces de sécurité qu'ils ont détectées dans l'exercice de leur mission de renseignement, dans le cas où la personne dont émane la menace fait l'objet d'un screening de sécurité.

EN CE QUI CONCERNE LA DISRUPTION PRIMAIRE

- Pour mettre en œuvre la recommandation relative à la disruption formulée par la Commission d'enquête parlementaire Attentats terroristes, l'adoption d'**une loi formelle** (*cf.* article 22 de la Constitution et article 8.2 de la CEDH) définissant les

[80] *Ibid.*, 40.

[81] *« Comparez-le à un sniper. 99 % du temps, vous êtes caché pour suivre une cible légitime, seulement 1 % du temps vous tirerez. Avec le moins de dommages collatéraux possible. Traduit dans le cybermonde : une fois que vous êtes entré dans un réseau, vous vous camouflez et vous attendez. Jusqu'à ce qu'à un moment donné, vous agissiez et neutralisiez temporairement une partie du réseau. Si votre adversaire utilise le réseau pour transporter des chars d'assaut d'un point A à un point B, par exemple. »* (traduction libre)

[82] AAP-06, ed. 2021, NATO Glossary of terms and definitions.

conditions de fond et de forme dans lesquelles la VSSE et le SGRS peuvent procéder à l'adoption et à la mise en œuvre de mesures de **disruption primaire**.

- Les points suivants méritent une attention particulière :
    - La réalisation d'un audit externe spécifique de la décision et de la mise en œuvre des mesures de disruption primaire.
    - Le volet 'mandataires politiques' dans la disruption primaire.
- Établir une liste exhaustive des mesures de disruption primaire par le **Conseil national de sécurité** pouvant être déployées par la VSSE, dans le respect des conditions légales d'application et de procédure.

EN CE QUI CONCERNE LES OPÉRATIONS CYBER DÉFENSIVES DU SGRS

- Définir **les processus de travail internes** de la composante Cyber Command du SGRS, y compris pour réglementer **les cyberopérations offensives**.